



VOLUME 19 ISSUE 1

KCJIS NEWS

FEBRUARY 2017

USER ACCOUNT PERMISSIONS

KIP BALLINGER IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

Last year, I wrote an article on User Account Review & Access Control. In it, I discussed the regular review of user accounts and their permissions. As I conduct KCJIS security audits, I continue to find agencies that have given their user accounts full administrative permissions. In most cases, it is administrative rights on the local machine (desktop admin account), but there are a few networks where users have been given administrative roles on the servers and/or domain.

Whether accidental through negligence or intentional, some 'standard' users are given full administrative privileges when their account is created. This typically happens when their account gets assigned as part of the desktop admin group, rather than the standard users group. A user with administrative rights has unrestricted access to either the local machine or domain, depending on how the computer is configured. If this full-permissions machine gets compromised, it is a free pass for the attacker. Giving end-users elevated access opens the door to malware and malicious attacks.

Accounts with admin rights can change other users' permission levels, even their ability to access their files. They can modify the audit logs, i.e., windows security, application, system logs, etc., by deleting events to cover their trail. Whether there is malicious intent or not, accidental or intentional, these issues are avoided by ensuring that users have permission levels commensurate with their job roles.

Privileged accounts are valid credentials used to gain access to systems. The difference is that they also provide elevated, non-restrictive access to the underlying platform that non-privileged user accounts don't have access to. There are risks to allowing users to run with local administrative rights on their computer. However, security flaws are not so critical if local administrative rights are not granted.

If malware executed code on the workstation as a 'standard' user, i.e., one with least privileges, the payload would be restricted to whatever tasks the user had permissions to perform. Typically, with only 'standard' user rights, malware would not be able to modify systems processes or services, registry entries, key system files, install malicious software, modify the system or cause permanent damage. If a user has local administrative rights, malicious software is able to disable the security enhancements that protect them. Besides security risks, there are threats to data confidentiality as it may be possible to gain access to other workstations and sensitive files, which they would not normally be allowed to access.

KCJIS Security Policy Section 5.5.2 (Access Enforcement) requires the information system to enforce assigned authorizations for controlling access to the system, as well as any contained information. The information system controls must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Access control policies (identity-based, role-based, and rule-based policies) and associated access enforcement mechanisms (access control lists, access control matrices, cryptography, etc.) must be employed by agencies to control access between users and objects (devices, files, records, processes, programs, domains, etc.) in the information system.

KCJIS Security Policy Section 5.5.2.1 (Least Privilege) requires each agency to enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. Each agency must implement least privilege based on specific duties, operations, or information systems as necessary in order to mitigate risk to Criminal Justice Information (CJI). This limits access to CJI to only authorized personnel with the need and the right to know.

As job roles change due to promotions, transfers, reassignments, etc., the performance of specified tasks may change as well, subsequently resulting in a change to that user's access privileges. Any changes to individual access privileges must be authorized and logs of access privilege changes must be maintained for a minimum of one year or at least equal to the agency's record retention policy - whichever is greater. All physical and logical access restrictions associated with these changes to the information system must be enforced.

INSIDE THIS ISSUE

USER ACCT PERMISSIONS 1-2

KIBRS DEADLINES 2

NEWS FROM HELP DESK 3

2017 KCJIS CONFERENCE 3

OFFENDER REG FAQ'S 4

UPCOMING KBI TRAINING 4

USER ACCOUNT PERMISSIONS, CONTINUED

KIP BALLINGER IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

KCJIS Security Policy 5.5.1 (Account Management) requires that each agency manage information system accounts. This includes establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency must validate information system accounts at least annually and document the validation process.

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJIS information and the modification of information systems, applications, services, and communication configurations allowing access to CJIS information.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. Each agency must identify authorized users of the information system and specify access rights and privileges.

Granting access to the information system must be based on a valid need-to-know/need-to-share, which is determined by assigned official duties and then, only after the satisfaction of all personnel security criteria. It would be prudent for a person who needs administrative access to a machine, to be given both an administrative account with a very robust (complex) password, which is only accessed when needed to make administrative changes on the computer, and also a "regular" user account, which is accessed for daily or routine use. In other words, you can reduce security risks on the local desktop by preventing users from using admin or root-level accounts when not performing admin tasks.

As a best practice, it is recommended that user accounts are reviewed more frequently than the annual minimum requirement. Regular reviews of agency user accounts and associated permissions (especially those with administrative privileges) will help to mitigate risk to the information systems and any data they contained therein. KCJIS Security Policy exists to mitigate these risks.

CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. To support information security practitioners and managers implement the CIS Critical Security Controls, SANS provide a number of resources and information security courses, which can be accessed through this link: <http://www.sans.org/critical-security-controls/>.

KIBRS REPORTING DEADLINES FOR REMAINING 2016 AND 2017 REPORTS

MITCH BEEMER, INCIDENT BASED REPORTING UNIT MANAGER KBI

The Incident Based Reporting (IBR) section at the Kansas Bureau of Investigation would like to remind all local law enforcement agencies of all upcoming deadlines in 2017. The IBR section does not guarantee inclusion in state and federal publications if your agency does not submit the required reports by the deadline.

March 1, 2017—Deadline to submit all 2016 Kansas Standard Offense and Arrest Reports to the KBI. This is the final deadline for submission of all 2016 reports. Data submitted by this deadline will be included in the FBI Crime in the United States publication and other annual statistic reports.

April 17, 2017—First quarter deadline. Submit January–March 2017 reports to the KBI headquarters.

July 17, 2017—Mid-year deadline. Submit January–June 2017 reports to the KBI headquarters.

October 16, 2017—Third quarter deadline. Submit January–September 2017 reports to the KBI headquarters.

January 15, 2018—Fourth quarter deadline. Submit January–December 2017 reports to the KBI headquarters.

February 22, 2018—Final deadline for submissions of all 2017 reports to the KBI. Data submitted by this deadline will be included in the FBI Crime in the United States publication and other annual statistic reports.

The Law Enforcement Officers Killed and Assault (LEOKA) reports, Supplemental Homicide Reports, and the Zero Reports are due by the 15th of the following month. For example, if an agency is sending data for the month of November, they should submit the November reports by December 15th. If the 15th falls on a weekend or holiday, the deadline is extended to the next business day.

For questions regarding submissions to IBR, please call the IBR duty line at (785) 296-4373.

NEWS FROM THE KBI HELP DESK**JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN III KBI****2017 Legislative Memo**

The 2017 Legislative Memo from the Division of Vehicles is available on the KCJIS Web Portal – Information – KS State Systems – KDOR section. This memo provides an overview of legislation decisions from the 2016 session impacting Kansas Law Enforcement agencies.

Did You Know?

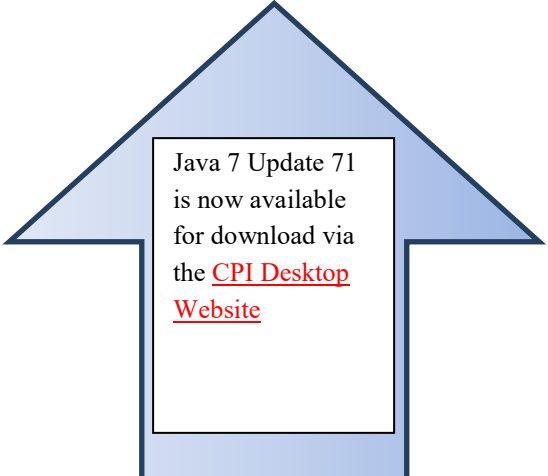
Did you know in OpenFox Messenger you can recall your last run transaction? Messenger maintains a brief history of the last transactions you have sent, and makes this history available to you on the mailbox window. For this and more OpenFox Messenger tips turn on the 'Tips of the Day' popup window when you first login to Messenger.

KCJIS User Group

At the January meeting the group received information about KS Warrant Conversion to NCIC from KBI IT staff. There was also discussion on formulating a SE KS User Group. Our next meeting is on May 4th, 2017 starting at 12:00PM in the Auditorium at the KBI Headquarters building in Topeka.

Federal Grant is Available

The Federal Edward Byrne Memorial Justice Assistance Grant may assist in funding CAD server upgrades. Official purpose areas and other consideration for use of this grant can be found on the [State of Kansas Grants Program](#) website. Application deadline is set for August 2017. The grant will begin on Oct 1, 2017 and end Sept 30, 2018.



Java 7 Update 71
is now available
for download via
the [CPI Desktop
Website](#)

2017 KCJIS CONFERENCE**GORDON LANSFORD, DIRECTOR KCJIS**

Save the Date!

2017 KCJIS Conference

When: June 4-6, 2017

Where: Ramada Inn West

605 SW Fairlawn

Topeka, KS 66606

The "Welcome" keynote will be presented by Joe Norwood, Kansas Secretary of Corrections and the "Future of Justice Systems" keynote will be presented by Sheriff Mike Milstead from South Dakota. "Sheriff Mike" is the Vice-Chair of the national Global Advisory Council (GAC). GAC provides advice and counsel to the US Attorney General on the use, standards, and future direction for integrated justice systems in the United States. He is also the driving force behind South Dakota's new "Connect South Dakota" program that has brought all law enforcement agencies together enabling users to query the whole state during investigations. We hope to see you there!

OFFENDER REGISTRATION FAQ'S**JENNIFER SLAGLE, PROGRAM CONSULTANT KBI**

Do you have questions about registered offenders? Here are some of the most common questions we receive from the public and law enforcement regarding registered offenders.

Q. Are there any restrictions on who an offender can or cannot be around, or where they can or cannot live, work, or go to school? For example, can sex offenders be around children? Can sex offenders be at parks or near schools?

A. Kansas does not have any laws that restrict who an offender can or cannot be around or where they can or cannot live, work, or go to school. However, there could be restrictions if an offender is on supervision (probation or parole).

Q. Why isn't an offender listed on the KBI public website?

A. There are several reasons why an offender may not be listed on the public website:

- Some juvenile offenders have restricted records, if ordered by the judge.
- Offenders who have moved to another state, are deported or deceased, and those who have satisfied their period of registration will not be on the public website.
- Offenders who have had their conviction expunged will not be on the public website; however they will still be required to register.
- Offenders convicted prior to the registration effective date for each offense will also not be on the public website (April 14, 1994 for most sex offenses; July 1, 1997 for most violent offenses; and July 1, 2007 for most drug offenses).

Q. Why would an offender's duration of registration be extended?

A. The duration of registration does not include any time an offender is incarcerated or fails to comply with the registration requirements of the Kansas Offender Registration Act. Therefore, those time periods will extend an offender's period of registration.

Q. What are some crimes that do not require registration, unless ordered by the court?

A. Unlawful voluntary sexual relations, vehicular homicide, involuntary manslaughter during commission of a DUI, and sale, distribution, or manufacturing of marijuana.

Q. A sex offender has a Facebook account. Is that allowed?

A. The Kansas Offender Registration Act does not prohibit the use of social networking sites by offenders. However, the social networking site itself could have a policy prohibiting sex offenders from having accounts. If discovered, those accounts would need to be reported directly to the social networking site for removal. Offenders are required to report their online identities to the registering agencies.

Q. If an offender was convicted in another state, are they required to register in Kansas?

A. Any person required to register in another state would be required to register in Kansas. The duration of registration would be the length of time required by the out of state jurisdiction or by the Kansas Offender Registration Act, whichever is longer.

Q. How can an offender be relieved of their duty to register?

A. There is no relief from their registration requirement.

Q. How would someone get in touch with the KBI Offender Registration Unit?

A. They may reach the KBI Offender Registration Unit by telephone at (785) 296-2841 or by email at registeredoffender@kbi.state.ks.us.

If you have additional questions, please feel free to contact the KBI Offender Registration Unit!

UPCOMING KBI TRAINING OPPORTUNITY**JESSICA CROWDER, PROGRAM CONSULTANT KBI**

The Kansas Bureau of Investigation will be providing training sessions March 1-2, 2017 at the KBI Headquarters in Topeka. Complementary sessions offered include Kansas Incident Based Reporting System (KIBRS), Criminal History Records, Case Inquiry, Rapsheet Differences, Offender Registration, 10 Print Fingerprint Identification, KsORT, and Central Message Switch/KCJIS Web Portal. For a class synopsis or to see the training schedule for the rest of 2017, click [here](#). If you wish to attend any of these training sessions, please register with the KBI receptionist at AnnexFrontDesk@kbi.state.ks.us or (785) 296-7404.



The KCJIS Newsletter is published in cooperation of the Kansas Criminal Justice Coordinating Council and KCJIS Committee

KCJCC Committee Members

Derek Schmidt
Attorney General
Chair

Sam Brownback
Governor
Vice-Chair

Kirk Thompson
Director
Kansas Bureau of Investigation

Justice Caleb Stegall
Chief Justice Designee

Joe Norwood
Secretary
Kansas Department of Corrections

Mark Bruce
Superintendent
Kansas Highway Patrol

KCJIS Committee Members

Capt. Justin Bramlett
Kansas Highway Patrol
Chair

Sec. Sarah Shipman
KS Department of Administration
Vice-Chair

Capt. Lance Royer
KS Sheriffs Association
Treasurer

Ed Klumpp
KS Association of Chiefs of Police
Immediate Past Chair

Leslie Moore
Kansas Bureau of Investigation

Harold Sass
KS Department of Corrections

Kelly O'Brien
Office of Judicial Administration

Pam Moses
KS Association of District Courts

Amber Norris
KS County and District Attorney Association

Bill Duggan
Lyon CO ECC
KS Assoc. of Public Communications Officers

KANSAS BUREAU OF INVESTIGATION

Jessica Crowder
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
(785) 296-8338
Jessica.Crowder@kbi.state.ks.us